



Online Safety Policy

2020-2023

Kings College Guildford

“An uncompromising commitment to excellence”

POLICY REVIEW AND AMENDMENT LOG

Statutory or Recommended: Statutory
Review frequency: Every 3 years
Next review date: August 2023

Reviewed By	Review Date	Reviewing Governor	Date Approved by Governing Body
Kate Carriett	July 2013	Matthew Armstrong	July 2013
Anna Wallis	June 2016		
Anna Wallis	July 2019	Bob Arnold	26/09/2019
Anna Wallis	August 2020	Mick Michell	08/12/2020

1. Aims

Kings College aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the Department's guidance on [protecting children from radicalisation](#). It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the principal to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The principal

The principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety as part of the safeguarding report to the governing board and principal.

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and SLT are informed so that they can be dealt with appropriately in line with this policy
- Ensuring that SLT are informed of any incidents of cyber-bullying so that they can be dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the principal.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff will find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 1). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendix 1.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the hours of 8am and 3pm. Mobile devices seen during these hours will be confiscated by staff.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct
- Data protection policy
- ICT and internet acceptable use policy

Appendix 1: Acceptable use agreement (pupils and parents/carers)

Kings College Student ICT & E-Safety User Guidance

Our Philosophy:

Information and Communication Technology is an integral part of education today. As a result, at Kings College we want to educate our students in the correct way to use this technology in order to gain the maximum benefit whilst remaining safe.

The following E-Safety Rules and Guidance are designed to help protect both students and the College by describing acceptable and unacceptable computer use. As a result, use of the internet, the College's learning platform and other related technologies can be monitored and logged and can be made available to teachers.

Acceptable Use

- Only using ICT systems in College for school purposes.
- Only logging on to the College network or learning platform using your own username and password.
- Accepting that you are responsible for all activity carried out under your username.
- Following the College's ICT security system and not revealing passwords to anyone and changing them regularly.
- Only using your College email address for College related work.
- Making sure that all ICT communications are responsible and sensible.
- Behaving responsibly when using the internet / learning platform.
- Being polite and respecting the views of others.
- Using discussion forums constructively.
- Ensuring that your online activity, both in College and outside College, will not cause distress or bring the College into disrepute.

Unacceptable Use

- Using ICT systems at College for personal gain or illegal purposes.
- Sending anonymous messages or chain mail.
- Giving out any personal information when using the College's learning platform.
- Arranging to meet someone unless this is part of a College project approved by a teacher.
- Deliberately browsing, downloading, uploading or forwarding material that could be considered offensive or illegal. If you accidentally come across any such material you will report it immediately to your teacher.
- Downloading or installing software on College technologies.
- Attempting to bypass the internet filtering systems.

I understand that these rules are designed to keep me safe and that if they are not followed, College sanctions will be applied and my parent/carer may be contacted. I understand that irresponsible use may result in loss of my network or internet access.

Kings College Mobile Phone Policy

Our Philosophy

- In line with many other Secondary schools, we will be banning the use of phones on the school site.
- Students will be able to bring phones to school as we understand that some may need them for communication to and from school.
- On the school site, phones must be switched off and in bags.
- If seen or heard anywhere on site, they will be confiscated by staff.
- Headphones will not be allowed as they would indicate and encourage phone use.

Why?

1. To improve the mental health and well-being of students in our care.
2. To improve concentration levels, focus, and therefore academic achievement.
3. To promote appropriate time and place for social mobile phone usage.

Sanctions

- For us to successfully implement this policy which will help to improve the well-being of the students in our care, it is important that we work together with students in order to help them break the cycle.
- Phones seen or heard during the school day will be confiscated by staff and stored securely by the reception team.
- No warnings or reminders will be given to students as the policy is clear.
- Students who choose to break the rules and refuse to hand over any phone seen will receive an additional sanction as per the behaviour policy.

Contact with home

- Students will be able to contact home via the Pastoral leader or members of the Leadership team.
- Parents who need to contact their children during school hours must do so via the school reception.

Appendix 2: Staff acceptable use agreement (staff, governors, volunteers and visitors)



ICT Code of Conduct 2020 - 2021

Kings College Guildford
“An uncompromising commitment to excellence”



This policy should be read alongside the GEP GDPR policy. There is also a simpler guide for staff in Section 7 of the staff handbook.

ICT and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in College. These policies and agreements are designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this document and adhere at all times to its contents. Any concerns or clarification should be discussed with the Kings College Guildford's e-safety co-ordinator.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDA's, digital cameras, e-mail, social networking and that ICT may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a College ICT system for a purpose not permitted by its owner.
- I will comply with the ICT system security and not disclose any passwords provided to me by the College or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the College's e-mail / internet / intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Principal or the Governing Body.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in College, taken off the College premises or accessed remotely. Personal data can only be taken out of College or accessed remotely when authorised by the Principal or Governing Body.
- I will not install any hardware or software without prior permission from Network Manager
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or the Principal.
- I will respect copyright and intellectual property rights.
- Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the College network / learning platform without the permission of the parent/carers, member of staff or the Principal.
- I will ensure my online activity, both in College and outside College, will not bring my professional role into disrepute.
- I will ensure that all electronic communications with parents, students and staff, including e-mail, IM and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will support the College's e-safety policy and help students to be safe and responsible in their use of ICT related technologies. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the e-safety Co-ordinator, the Child Protection Liaison Officer or the Principal.
- I understand that sanctions for disregarding any of the above will be in line with the College's disciplinary procedures and serious infringements may be referred to the police.
- I understand that the school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Mobile Device Guidance for Staff, Governors or Visitors

Mobile Phone Acceptable Use Policy

The widespread ownership of mobile phones requires that school administrators, teachers, parents and carers take steps to ensure that mobile phones are used responsibly at school. This Acceptable Use Policy has been designed to ensure that potential issues involving mobile phones can be clearly identified and addressed.

General Use of Mobile Phones

- Mobile phones and personally owned devices brought into College are the responsibility of the device owner. The College accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- The Bluetooth functionality of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally owned mobile devices without the prior consent of the person or people concerned.

Staff Acceptable Use of Mobile Phones

- In line with our 'Phone Free School' policy for students, staff use of mobile phones during the College day should be limited. Mobile phones will be kept out of sight during classroom lessons, assemblies, whilst moving through the corridors and when in the library.
- During free time only, and away from students, staff will be permitted to use mobile devices.
- Mobile phones should not be used in any manner or in any location that could cause disruption to the normal routine of the College.
- Staff should ensure that their phones are PIN protected in case of loss or theft. This is to protect the staff from their number falling into the wrong hands.
- When on a College trip staff will be issued with a College mobile where contact with students, parents or carers is required. If staff need to contact parents or carers whilst at College they will use a College based landline in departments or College offices.

Governor and Visitor Acceptable Use of Mobile Phones

- Governors and Visitors use of mobile phones on the College site and during the College day should be limited. Mobile phones will be kept out of sight whilst in classrooms, moving through the corridors and when in the library.
- If Governors and Visitors need to use mobile phones they are to do so in privacy and away from students.
- Mobile phones should not be used in any manner or in any location that could cause disruption to the normal routine of the College.
- Governors and Visitors should ensure that their phones are PIN protected in case of loss or theft. This is to protect them from their number falling into the wrong hands

Acceptable Use Agreement

This Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that staff will have good access to digital technologies to enhance their teaching and will, in return, expect staff to agree to be responsible users.

Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

I understand that the following provides guidance to staff on the appropriate use of the school network. However, this is not a definitive list and staff should use their judgement to ensure the safety of all.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of dangers associated with contact with strangers when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line or any other information by which I or my location could be identified (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, location etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. (Please do not delete so that this can be used should evidence be required)

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, personal financial gain, political purposes, advertising or video broadcasting (e.g. YouTube), unless I have permission to do so.
- I will not search for, create, transmit, download or print inappropriate or illegal web content such as but not limited to any offensive, obscene, pornographic or indecent images, data or other material, or any data capable of being resolved into pornographic or indecent images or material; separately

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission. Copyright and intellectual property rights must be respected.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. As messages may be forwarded, messages should be regarded as public property.
- I will not take or distribute images of anyone without their permission.
- I will not send mass messages or anonymous messages.
- I am aware that the school reserves the right to monitor all my electronic communications accessed via school systems. (RIP Act 2000)

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission and I understand that, if I do use my own devices in the school I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any program or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email or message, or if I have any concerns about the validity of the email or message (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, and, in the event of illegal activities, involvement of the police.

Bring Your Own Device Terms and Conditions of Use

Note : Kings College Guildford cannot guarantee the speed of access to the internet.

- I understand that my device should have an appropriate level of security and that anti-virus is my responsibility.
- I will ensure my personal device is insured against theft, loss and damage.
- I am aware that in order to prevent unauthorised access to my device I should have a password with auto-lock.
- I understand that my personal device is my responsibility.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in this document. If you do not sign and return this agreement, access will not be granted to school systems and devices. If you breach any of these terms and conditions of use, your permission to use Kings College IT services will be terminated.

Agreement Form

This form relates to the 'ICT Code of Conduct', 'Mobile Device Guidance for Staff, Governors or Visitors', 'Acceptable Use Agreement' and the 'Acceptable Use Policy Agreement'

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school
- I use my own equipment out of the school / academy in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name

Signed

Date

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	Date:
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

